REMARKS

Applicant has carefully studied the outstanding Office Action. The present response is intended to be fully responsive to all points of rejection raised by the Examiner and is believed to place the application in condition for allowance. Favorable reconsideration and allowance of the application is respectfully requested.

Claims 1 - 10 are pending in this case. Claims 1 - 10 have been rejected under 35 U.S.C. § 103. Independent claims 1, 5, 8-10 and dependent claims 2-4, 6-7 have been amended. New claims 11-19 have been added.

Personal Interview

Applicant wishes to thank Examiner Nguyen Nguyen and Supervisory Examiner Hassan Kizou for granting a personal interview on January 11, 1999.

35 U.S.C. § 103 Rejections - Kuznetsov/Francisco

The Examiner has rejected claims 1 - 11 under 35 U.S.C. § 103(a) as being unpatentable over Kuznetsov ('649) in view of Francisco ('147).

Kuznetsov teaches a personal computer subsystem having a hardware module and protection software that is designed to protect files on a personal computer from inadvertent or intentional distortion such as from computer viruses. The hardware module is connected to the computer system buses and the software includes a kernel that protects an access path to the hard disk controller. The only permissible path utilizes the computer's operating system, modular device driver and BIOS. All other accesses are blocked.

While continuing to traverse the Examiner's rejections, Applicant, in order to expedite the prosecution, has chosen to clarify and emphasize the crucial distinctions between the present invention and the devices of the patents cited by the Examiner. Specifically, claim 1 has been amended to include a method of creating a secure sandbox around both a monitored application and one or more software components associated therewith in accordance with a predetermined security policy, the method comprising the steps of intercepting a selected set of application programming interface (API) function calls issued by the monitored application by replacing the addresses of all API functions to be intercepted in an import data table associated with the monitored application with addresses of security monitor functions, each security monitor function associated with a different API function, intercepting API function calls issued by the software component by replacing the addresses of API functions to be intercepted in an import data table associated with the software

A

component with addresses of stub functions, each stub function operative to call a security monitor function associated with a different API function, intercepting non-API function calls issued by the software component by replacing the addresses of non-API functions to be intercepted in an import data table associated with the software component with addresses of stub functions, each stub function operative to call a security monitor function associated with a different non-API function, creating a call chain operative to permit distinguishing between function calls made by the software component from function calls made by the monitored application, blocking intercepted API calls that are forbidden according to the security policy and allowing intercepted API calls that are permitted according to the security policy.

It is submitted that Kuznetsov, Francisco Olkin and Ault each fail to disclose the steps of intercepting a selected set of API functions calls issued by the monitored application, intercepting API functions call issued by the software component, intercepting non-API function calls issued by the software component, creating a call chain to distinguish between function calls made by the software component from function calls made by the monitored application, and only allowing API calls that are permitted according to the security policy.

Kuznetsov teaches a hardware method of providing security only for access to a hard disk drive.

In contrast, the method of the present invention utilizes software only to intercept API and non-API function calls from the monitored application and the software component.

It is believed that amended independent claims 1, 5, 8-10 and 16 overcome the Examiner's § 103 rejection based on the Kuznetsov reference. In addition, it is believed that amended dependent claims 2-4, 6-7 and new dependent claims 11-15, 17-19 also overcome the Examiner's rejection based on § 103 grounds. The Examiner is respectfully requested to withdraw the rejection based on § 103.

In view of the above amendments and remarks, it is respectfully submitted that independent claims 1, 5, 8-10, 16 and dependent claims 2-4, 6-7, 11-15, 17-19 are now in condition for allowance. Prompt notice of allowance is respectfully solicited.

Respectfully submitted,

By: _____

S. Peter Ludwig
Registration No. 25,351
Attorney for Applicant(s)

DARBY & DARBY PC
805 Third Avenue
New York, NY 10022-7513
(212) 527-7700